

PCT
 WELTORGANISATION FÜR GEISTIGES EIGENTUM
 Internationales Büro
 INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE
 INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)



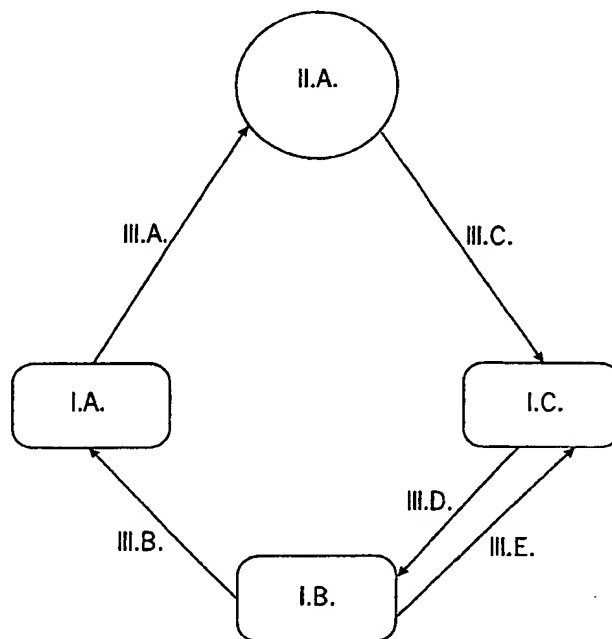
(51) Internationale Patentklassifikation ⁷ : G07F 7/10	A1	(11) Internationale Veröffentlichungsnummer: WO 00/39758 (43) Internationales Veröffentlichungsdatum: 6. Juli 2000 (06.07.00)
(21) Internationales Aktenzeichen: PCT/EP99/09531 (22) Internationales Anmeldedatum: 6. Dezember 1999 (06.12.99) (30) Prioritätsdaten: 198 60 203.0 24. Dezember 1998 (24.12.98) DE (71) Anmelder (für alle Bestimmungsstaaten ausser US): DEUTSCHE TELEKOM AG [DE/DE]; Friedrich-Ebert-Allee 140, D-53113 Bonn (DE). (72) Erfinder; und (75) Erfinder/Anmelder (nur für US): KORST, Uwe, K., H. [DE/DE]; Talstrasse 14, D-64625 Bensheim (DE). WANKO, Clemens [DE/DE]; Tilsiter Strasse 6, D-63322 Rödermark (DE). (74) Gemeinsamer Vertreter: DEUTSCHE TELEKOM AG; Patentabteilung PA1, D-64307 Darmstadt (DE).		(81) Bestimmungsstaaten: HU, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Veröffentlicht <i>Mit internationalem Recherchenbericht.</i>

(54) Title: METHOD FOR THE SECURE HANDLING OF MONEY OR UNITS OF VALUE WITH PRE-PAID DATA CARRIERS

(54) Bezeichnung: VERFAHREN FÜR DIE SICHERE HANDHABUNG VON GELD- ODER WERTEEINHEITEN MIT VORAUS-BEZAHLTEN DATENTRÄGERN

(57) Abstract

The invention relates to a payment method in public telecommunications systems by means of pre-paid chip cards, especially in the form of memory chip cards or microprocessor chip cards. The card value is managed in a central background system and the communication is entirely controlled by said background system. According to the invention, a chip, for example a telephone card, is personalised, i.e. provided with a definite identification number of identification characteristic, by the card provider (I A). A value is assigned to the identification characteristic. Said value, however, is not saved on the chip of the data carrier. The value is made available, together with the identification characteristic, for a background system (I B) via a communications channel (III B). The identification characteristic and the value are saved in a data bank in the communications channel. The identification characteristic is provided with the label "not cleared". Said label is cancelled by the data bank just before the respective card is actually sold which makes the value ready for debiting in the background system. A customer (2) can use such a chip card (II A) in a communications terminal (I C) which is designed therefor, whereby only the identification characteristic is read out from the card in order to forward said identification characteristic to the background system (I B) and request a debit (III D). The background system (I B) can release the original value that has been assigned in the personalisation process, allocate said value to the identification characteristic and confirm the debit (III E). The communications link is directly created and controlled by the background system. A link can thus be cut after debiting of the entire card value in the data bank of the background system (I B) using said background system (I B).



(57) Zusammenfassung

Es wird ein Verfahren für die Bezahlung in der öffentlichen Telekommunikation mittels vorausbezahlten Chipkarten, insbesondere in Form von Speicherchipkarten oder Mikroprozessorchipkarten beschrieben, wobei der Kartenwert in einem zentralen Hintergrundsystem verwaltet wird und die Kommunikation vollständig durch das Hintergrundsystem gesteuert wird. Dabei wird ein Chip, zum Beispiel einer Telefonkarte, durch den Kartenausgeber (I A) personalisiert, das heißt mit einer eindeutigen Identifikationsnummer bzw. einem Identifikationsmerkmal versehen. Dem Identifikationsmerkmal wird ein Wert zugeordnet, der jedoch nicht auf dem Chip des Datenträgers gespeichert wird. Der Wert wird zusammen mit dem Identifikationsmerkmal einem Hintergrundsystem (I B) über einen Kommunikationsweg (III B) verfügbar gemacht. Dort wird das Identifikationsmerkmal zusammen mit dem Wert in einer Datenbank gespeichert und zunächst mit dem Vermerk "nicht freigeschaltet" versehen. Unmittelbar vor dem eigentlichen Verkauf der jeweiligen Karte wird dieser Vermerk in der Datenbank entfernt und damit steht der Wert im Hintergrundsystem zur Abbuchung bereit. Ein Kunde (2) kann eine derartige Chipkarte (II A) an einem hierfür vorgesehenen öffentlichen Kommunikationsterminal (I C) nutzen, wobei lediglich das Identifikationsmerkmal aus der Karte ausgelesen wird, um es an das Hintergrundsystem (I B) weiterzuleiten und eine Buchungsanfrage (III D) durchzuführen. Das Hintergrundsystem (I B) kann nun dem Identifikationsmerkmal seinen ursprünglichen bei der Personalisierung zugeordneten Wert freigeben und die Buchungsbestätigung (III E) durchführen. Die Kommunikationsverbindung wird hierbei unmittelbar durch das Hintergrundsystem vermittelt und kontrolliert. Damit kann eine Verbindung nach Abbuchung des vollständigen Kartenwertes in der Datenbank des Hintergrundsystems (I B) durch dasselbe getrennt werden.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidshan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

**VERFAHREN FÜR DIE SICHERE HANDHABUNG VON GELD- ODER
WERTEEINHEITEN MIT VORAUSBEZAHLTEN DATENTRÄGERN**

BESCHREIBUNG

5 Die Erfindung betrifft ein Verfahren für die sichere Handhabung von Geld- oder Werteeinheiten mit vorausbezahlten Datenträgern nach dem Oberbegriff des Patentanspruchs 1.

10 Konzepte für das Betreiben von elektronischen Geldbörsen auf Chipkarten befinden sich bereits seit einigen Jahren sowohl in der Entwicklung als auch im Einsatz. Sie beinhalten neben der Technik der Chipkarte in den meisten Fällen auch die Sicherheitstechnik für das Zusammenwirken von Chipkarte und Rechner- und Übertragungssystemen sowie die Abrechnung der
15 mit der Chipkarte vorgenommenen Transaktionen. Sowohl national als auch international wurden bereits zahlreiche Konzepte vorgestellt. In einigen Ländern sind elektronische Geldbörsensysteme eingesetzt, wie zum Beispiel

- 20 - Feldversuch Eisenstadt, Österreich, seit Dezember 1994
- Avantcard - in Finnland
- Danmond Konzept in Dänemark
- Mondex, in Swinton, England
- darüberhinaus wird unter CIN TC224 WG10 eine
25 "intersect electronic purse" (branchenübergreifende elektronische Geldbörse) standardisiert.

In diesen bekannten Systemen wird grundsätzlich folgendes Verfahren verwendet:

30 Der erste Schritt ist das Laden von geldwerten Einheiten in die Chipkarte, wobei der Gegenwert, den der Karteninhaber in bar oder auch bargeldlos bezahlen muß, auf einem sogenannten "Pool-Konto" - des Börsenbetreibers hinterlegt wird. Beahlt
35 ein Karteninhaber anschließend mit seiner Chipkarte, werden geldwerte Einheiten aus der elektronischen Geldbörse herausgebucht und mit Hilfe eines Sicherheitsmoduls zum Terminal des Serviceanbieters übertragen. Dort werden die

eingenommenen geldwerten Einheiten entweder zu einem Betrag akkumuliert und mit dem Börsenbetreiber abgerechnet oder aber jeder einzelne Bezahlvorgang wird beim Börsenbetreiber zur Abrechnung eingereicht. Akkumulierte Beträge oder
5 einzelne Datensätze werden entweder auf einer sogenannten Händlerkarte gesammelt, die der Serviceanbieter einreichen muß oder mit einem entsprechenden ausgerüsteten Terminal online an eine Abrechnungsstelle übertragen.

10 Weiterhin sind elektronische Geldbörsenanwendungen bekannt, die auf einer Mikroprozessorkarte realisiert sind. Bei Mikroprozessoranwendungen erfolgt die Steuerung der Anwendung durch ein Chipkartenbetriebssystem, wie es
15 beispielsweise im Standard prEN726-3 definiert ist. Auch diese Anwendung zeichnet sich dadurch aus, daß auf der Karte Geldbeträge gespeichert werden, die bei jeder Abbuchung um einen festgelegten Betrag reduziert werden. Der Vorteil der bekannten Mikroprozessorkarten gegenüber den bekannten
20 Speicherkarten besteht darin, daß die Mikroprozessorkarten prüfen können, ob das abbuchende System authentisch ist oder umgekehrt. Diese Überprüfung ist bei einer Speicherchipkarte nicht möglich. Außerdem sind ähnliche Systeme und Verfahren durch die
US-A-4,859,837, WO-A-90 15 382 und die DE 42 43 851 A1
25 realisiert. Außerdem ist noch ein Verfahren zur Transaktionskontrolle elektronischer Geldbörsensysteme in der DE 196 04 876 C1 beschrieben.

Die größte Verbreitung haben die Telefonkarten.

30 Telefonkarten sind Speicherchipkarten mit einem Identifikationsbereich und mindestens einem Zählerbereich. Außerdem ist unter der Bezeichnung Virtual Calling Card (VCC) in den USA ein Dienst eingeführt worden, der es dem Kunden ermöglicht, durch Angabe einer
35 Zugangskennung in Verbindung mit einer PIN (Personal Identification Number), von jedem beliebigen Telefon aus zu telefonieren. Diese sogenannten Calling Card-Systeme basieren in der Regel auf einer zentralen Steuereinheit mit

entsprechender Datenbank bzw. einem Zentralrechner. Die
Gebührenabrechnung erfolgt dabei über ein dem Kunden
zugeordnetes Konto. Dieser Dienst gewinnt zunehmend auch in
Europa an Bedeutung. So ist zum Beispiel in "Deutsche
5 Telekom AG - Vision", Februar 1995, Seiten 44 und 45, die T-
Card mit Connect Service der Deutschen Telekom beschrieben.

In diesem Artikel ist auch ausgeführt, daß sich das
Leistungsspektrum von der Telefonkarte bis hin zur
10 Kreditkarte erstreckt. Zum Beispiel ist im Absatz 4.1.2.1.,
ab Seite 61 des Buches "Chipkarten als Werkzeug" von
Beutelsberger, Kersten und Pfau beschrieben, wie
Speicherchipkarten auf Authentizität durch Anwendung
bekannter Challenge-Response Verfahren geprüft werden. Mit
15 diesen Chipkarten ist es mit Hilfe eines Terminals bzw.
eines Kartenlesers möglich, die Karten zu identifizieren und
auf Plausibilität zu prüfen. In einem im Terminal
eingebauten Sicherheitsmodul wird eine Authentifikation
vorgenommen.

20 Weiterhin ist ein Verfahren zum Prüfen von
Speicherchipkarten durch die DE 196 04 349 A1 bekannt, das
eine zwei- oder mehrfache Authentifikation mit Hilfe
kryptographischer Funktionen und mit Hilfe eines Terminals
25 ermöglicht.

Der Nachteil der heute überwiegend benutzten Verfahren und
Systeme besteht darin, daß der jeweilige Wert bzw. die
Werteinheiten auf dem Datenträger, zum Beispiel der
30 Chipkarte oder der Mikroprozessorkarte gespeichert ist/sind.
Die Endgeräte erkennen den auf dem Datenträger gespeicherten
Wert und erniedrigen entsprechend des Preises einer
gekauften bzw. verkauften Dienstleistung den Wert auf dem
Datenträger. Aufgrund der großen Anzahl von vorausbezahlten
35 Datenträgern, die in Umlauf gebracht werden, wird in der
Regel auf das Führen eines sogenannten Schattenkontos bzw.
Schattensaldos in den Endgeräten und/oder deren
Hintergrundsystemen verzichtet. Damit ist den Endgeräten und

deren Hintergrundsystemen die Verifizierung, zum Beispiel des Sollwertes, eines sich in Gebrauch befindlichen Datenträgers nicht möglich. Durch Manipulation oder Fälschung des Datenträgers können somit Geld- oder Werteeinheiten erzeugt werden, die eigentlich dem Betreiber eines Buchungssystems zustünden. Die hierdurch für die Betreiber entstehenden Schäden werden derzeit weltweit monatlich auf einen zweistelligen Millionenbetrag geschätzt.

Die Systeme mit Schattenkonten bzw. Schattensalden haben den entscheidenden Nachteil, daß große Datenmengen im System übertragen werden müssen. Weiterhin sind viele Endgeräte nicht online angeschlossen, sondern übertragen erst mit einer Zeitverzögerung die Datensätze. Manipulationen sind somit nicht sofort erkennbar.

Der Erfindung liegt deshalb die Aufgabe zugrunde, ein Verfahren zur sicheren Handhabung von Geld- oder Werteeinheiten mit vorausbezahlten Datenträgern, wie zum Beispiel Chipkarten, Magnetstreifenkarten oder ähnliches, in elektronischen Buchungssystemen wie Telefonkartensystemen, Geldbörsensystemen und ähnliches zu schaffen, das eine Kartenmanipulation wertlos macht und das den gegebenenfalls hohen Datenübertragungsaufwand bei den bekannten Systemen reduziert.

Die erfindungsgemäße Lösung der Aufgabe ist im Kennzeichen des Patentanspruchs 1 charakterisiert.

Weitere Lösungen sind in dem jeweils kennzeichnenden Teil der Patentansprüche 2 bis 7 angegeben.

Durch das erfindungsgemäße Verfahren ist ein potentieller Betrüger bzw. Angreifer gezwungen, das Hintergrundsystem des Betreibers zu manipulieren oder zu scannen, das heißt durchprobieren verschiedener Erkennungsmuster, um an den Gegenwert eines jeweiligen Datenträgers bzw. einer Chipkarte zu gelangen. Dies ist für den Betrüger wesentlich

5 schwieriger in der Durchführung als die Manipulation des
jeweiligen Datenträgers in Form einer Speicherchipkarte oder
einer Mikroprozessorchipkarte. Für den Betreiber hingegen
ist ein zentrales Hintergrundsystem in gesicherter Umgebung
wesentlich einfacher gegen unerlaubte Zugriffe zu schützen.
Findet zum Beispiel ein Betrüger durch Scannen ein
Erkennungsmuster heraus, so steht ihm lediglich der
Gegenwert dieses einen Datenträgers bzw. Erkennungsmusters
zur Verfügung. Das Scannen des nächsten Erkennungsmusters
10 erfordert von ihm wieder den gleichen hohen Aufwand. Wichtig
ist, daß die Manipulation der Datenträger selbst durch
dieses Verfahren zwecklos wird. Der Wert einer Kopie bzw.
einer Simulation von Datenträgern würde sich auch nur auf
den jeweiligen geringen aktuellen Wert des einzelnen
15 Datenträgers beschränken. Außerdem hat das vorliegende
Verfahren noch den Vorteil, daß es den hohen
Datenübertragungsaufwand der bisher bekannten Verfahren mit
Schattenkonten reduziert. Die Reaktionszeiten auf erkannte
Sicherheitsprobleme im Hintergrundsystem werden im Vergleich
20 zu dem bisherigen Verfahren wesentlich kürzer und die
Zuordnung von Leistungsmerkmalen zur Identifikation kann
jetzt im zentralen Rechner oder in der zentralen
Steuereinheit des Hintergrundsystems vorgenommen werden.

25 Weitere Vorteile, Merkmale und Anwendungsmöglichkeiten der
vorliegenden Erfindung, sowohl für den Netzbetreiber und den
Diensteanbieter als auch für den Benutzer des Datenträgers
ergeben sich aus der nachfolgenden Beschreibung in
Verbindung mit dem in der Zeichnung dargestellten
30 Ausführungsbeispielen.

Die Erfindung wird im folgenden anhand von in der Zeichnung
dargestellten Ausführungsbeispielen näher beschrieben. In
der Beschreibung, in den Patentansprüchen, der
35 Zusammenfassung und in der Zeichnung werden die in der
hinten angeführten Liste der Bezugszeichen verwendeten
Begriffe und zugeordneten Bezugszeichen verwendet.

In der Zeichnung bedeutet:

Fig. 1 ein prinzipielles Operationsdiagramm des erfindungsgemäßen Verfahrens.

5

Bevor die detaillierte Funktionsweise und Wirkungsweise des erfindungsgemäßen Verfahrens anhand Fig. 1 erklärt wird, soll zunächst eine Beschreibung der grundsätzlichen Wirkungsweise und Verfahrensschritte folgen.

10

Ein Kunde erwirbt eine Telefonkarte. Die Telefonkarte enthält zum Beispiel in einem Chip gespeichert lediglich die Telefonkarten ID 12345... . Führt der Kunde die Karte in ein Kartentelefon ein, so liest dieses Telefon die ID aus und stellt eine Verbindung zum Hintergrundsystem her. Über diese Verbindung wird dem Hintergrundsystem die ID übermittelt. Das Hintergrundsystem kann daraufhin der ID einen Wert in Form von Einheiten oder DM zuordnen. Der Kunde beginnt nun mit der Wahl einer Telefonnummer. Die Wahlinformationen werden jedoch nicht vom Kartentelefon ausgewertet, sondern lediglich von dort an das Hintergrundsystem weitergeleitet. Hier werden die Wahlinformationen ausgewertet, die Verbindung wird entsprechend des noch vorhandenen Guthabens aufgebaut und bei Erreichen des Guthabenwertes Null wieder getrennt.

15

20

25

Durch die Steuerung der Verbindung mittels eines zentralen Hintergrundsystems (ähnlich dem eines Calling Card-Systems) können fast alle erdenklichen Leistungen angeboten und einfach (da zentral) administriert und weiterentwickelt werden.

30

Weiterhin kann der ID zum Beispiel ein bestimmtes Tarifmodell zugeordnet werden (wurde die Karte = ID zum Beispiel im Rahmen einer Sonderaktion verkauft, mit der besonders günstige Verbindungskonditionen verknüpft waren, so kann dies durch Zuordnung eines entsprechenden Tarifmodells umgesetzt werden). Auf diese Art ist die

35

Verknüpfung verschiedenster Leistungsmerkmale und Dienstleistungen möglich.

- 5 Durch das hier angegebene Verfahren ist es möglich, daß der außer Reichweite des jeweiligen Betreibers befindliche Datenträger des Nutzers bzw. Kunden, der sich hierdurch in einer unsicheren Umgebung befindet, nicht mehr den Geld- oder Einheitenwert enthält, sondern nur noch ein eindeutiges Erkennungsmuster, zum Beispiel eine Seriennummer, ein
- 10 Kryptogramm, einen Kryptoschlüssel oder Äquivalentes. Das Erkennungsmuster wird vom Endgerät bei einem Nutzungsvorgang abgefragt. Der Datenträger identifiziert sich anhand des Erkennungsmusters einem Endgerät und seinem Hintergrundsystem bzw. Hintergrundsystemen gegenüber
- 15 eindeutig. Der dem Datenträger zugeordnete Geld- oder Einheitenwert wird entsprechend einer verkauften oder gekauften Dienstleistung in den Hintergrundsystemen der Betreiber erniedrigt.
- 20 Um einem Angreifer bzw. potentiellen Betrüger den Zugang zu einem Erkennungsmuster, zum Beispiel durch Scannen, zu erschweren, ist das Erkennungsmuster möglichst komplex zu wählen und es kann überdies auch auf dem Datenträger kryptographisch gesichert abgelegt werden.
- 25 Das Erkennungsmuster ist als sogenannter öffentlicher kryptographischer Schlüssel ausgeführt, der für jeden Datenträger jeweils nur einmal existiert. Ein Endgerät/Hintergrundsystem sendet dem Datenträger eine
- 30 sogenannte Challenge, die durch den Datenträger selbst mittels des auf dem Datenträger hinterlegten kryptographischen Schlüssel verschlüsselt wird. Das Ergebnis ist die sogenannte Antwort (Response). Sie wird dem Hintergrundsystem bzw. Endgerät des Betreibers
- 35 zurückgesendet. Der in den Hintergrundsystemen des Betreibers hinterlegte sogenannte geheime Schlüssel zu genau diesem einen Datenträger wird vom Hintergrundsystem zur Entschlüsselung der Response verwendet. Stimmen Challenge

und Response überein, dann ist der Datenträger authentisch. Außerdem ist eine zusätzliche Führung der Geld- und Werteeinheiten, gegebenenfalls kryptographisch gesichert, auf dem Datenträger zur Durchführung einer Plausibilitätskontrolle möglich.

In dem in Fig. 1 dargestellten prinzipiellen Verfahrensdiagramm finden die in der öffentlichen Telekommunikation üblichen Chipkarten in Form von Speicherchipkarten bzw. Mikroprozessorchipkarten Anwendung. Besondere Sicherheitseigenschaften dieser Chipkarten sind nicht erforderlich. Es ist lediglich bei der Personalisierung der Chipkarten zu beachten, daß das Identifikationsmerkmal zufällig aus einem um mehrere Dimensionen größeren Wertebereich gewählt wird. Beispiel: Herausgegebene Karten insgesamt = 10^6 Stück, Wertebereich = 10^{12} , woraus sich die Länge der Kartennummer zu 12 Stellen ergibt. Das Diagramm nach Fig. 1 ist grundsätzlich in die Telekommunikationsinfrastruktur I, den Kundenbereich II und in die Kommunikationswege III unterteilt.

Das Verfahren läuft nun wie folgt ab: Ein Speicher- bzw. Mikroprozessorchip einer zum Beispiel Telefonkarte wird durch den Kartenausgeber I A personalisiert, das heißt mit einem eindeutigen Identifikationsmerkmal, zum Beispiel einer Kartennummer, versehen. Diesem Identifikationsmerkmal wird ein Wert (zum Beispiel x DM oder x Einheiten) zugeordnet, der jedoch nicht im Chip gespeichert bzw. hinterlegt wird. Der Wert wird zusammen mit dem Identifikationsmerkmal dem Hitnergrundsystem I B über den Kommunikationsweg III B verfügbar gemacht. Dort wird das Identifikationsmerkmal zusammen mit dem Wert in einer Datenbank gespeichert. Dabei erfolgt die Speicherung zunächst mit dem Vermerk "nicht freigeschaltet".

Unmittelbar vor dem Verkauf der Telefonkarte durch den Kartenausgeber wird der Vermerk "nicht freigeschaltet" in

der Datenbank des Hintergrundsystems I B entfernt. Der Wert der jeweiligen Karte steht damit im Hintergrundsystem I B zur Abbuchung bereit. Nutzt nun ein Kunde II eine derartige Chipkarte II A an einem hierfür vorgesehenen öffentlichen Kommunikationsterminal I C, dann liest das Telekommunikationsterminal lediglich das Identifikationsmerkmal aus der Karte aus, um es an das Hintergrundsystem I B weiterzuleiten, das heißt es führt eine Prüfungsanfrage III D aus. Das Hintergrundsystem fügt nun dem Identifikationsmerkmal seinen ursprünglich bei der Personalisierung zugeordneten Wert zu und bei ausreichenden Guthaben wird die Kommunikation freigegeben, das heißt es folgt eine Buchungsbestätigung III E. Die Kommunikationsverbindung wird hierbei unmittelbar durch das Hintergrundsystem I B vermittelt und kontrolliert. Damit kann eine Verbindung nach Abbuchung des vollständigen Kartenwertes in der Datenbank des Hintergrundsystems I B durch dasselbe getrennt werden.

Liste der Bezugszeichen

- | | | |
|----|-----|--|
| | I | Telekommunikationsinfrastruktur |
| | A | Kartenherausgeber (Chipkartenpersonalisierung) |
| 5 | B | Hintergrundsystem (mit Datenbank) |
| | C | Kommunikationsterminal oder Endgerät |
| | | |
| | II | Kunde |
| | A | Chipkarte oder Datenträger |
| 10 | | |
| | III | Kommunikationswege |
| | A | Chipkartenausgabe |
| | B | Übermittlung Personalisierungsdaten |
| | C | Chipkartennutzung |
| 15 | D | Buchungsanfrage |
| | E | Buchungsbestätigung |

PATENTANSPRÜCHE

1. Verfahren zur sicheren Behandlung bzw. Handhabung von Geld- oder Werteinheiten mit vorausbezahlten Datenträgern, wie zum Beispiel Chipkarten oder Magnetstreifenkarten in elektronischen Buchungssystemen für zum Beispiel Telefonkartensysteme, Geldbörsensysteme oder äquivalente Systeme, **dadurch gekennzeichnet,**

daß der von einem Kunden oder Nutzer vorausbezahlte Datenträger (II A) nur noch ein eindeutiges Erkennungsmuster bzw. Identifikationsmerkmal, wie zum Beispiel eine Seriennummer, ein Kryptogramm, einen Kryptoschlüssel oder ähnliches aufweist, und vom Kartenausgeber (I A) personalisiert wird,

daß dem Erkennungsmuster bzw. Identifikationsmerkmal ein Wert zugeordnet wird, die beide zusammen einem Hintergrundsystem (I B) über einen Kommunikationsweg (III B) zur Übermittlung der Personalisierungsdaten verfügbar gemacht werden, dort gespeichert und zunächst mit einem Vermerk "nicht freigeschaltet" versehen werden,

daß unmittelbar vor oder beim Verkauf des zugehörigen Datenträgers der Vermerk in der Datenbank des Hintergrundsystems (I B) entfernt wird,

daß dieses Erkennungsmuster einem Endgerät (II C) und/oder seinem(n) Hintergrundsystem bzw. -systemen bei einem Nutzungsvorgang automatisch ohne Zutun des Nutzers zugeführt wird, indem es abgefragt wird, wobei die Eingabe weiterer Identifikationsmerkmale durch den Nutzer optional möglich ist,

daß der Datenträger (II A) anhand des Erkennungsmusters sich eindeutig dem Endgerät und/oder seinem/seinen Hintergrundsystem(en) (I B) gegenüber identifiziert und

5 daß dann darauffolgend der dem Datenträger (II A) zugeordnete Geld- oder Einheitenwert entsprechend einer verkauften bzw. gekauften Dienstleistung im Hintergrundsystem (I B) des Betreibers automatisch verringert und verwaltet wird.

10

2. Verfahren nach Patentanspruch 1, **dadurch gekennzeichnet,**

15

daß das Hintergrundsystem (I B) die Kommunikationsverbindung unmittelbar vermittelt und kontrolliert,

20

daß das Erkennungsmuster des Datenträgers (II A) ein sogenannter öffentlicher kryptographischer Schlüssel ist, der für jeden Datenträger jeweils nur einmal existiert und

daß dem Schlüssel bzw. einer ID ein bestimmtes Tarifmodell zugeordnet wird.

25

3. Verfahren nach Patentanspruch 2, **dadurch gekennzeichnet,**

daß das jeweilige Buchungssystem den zugehörigen geheimen Schlüssel kennt und den Datenträger anhand eines Challenge/Response-Verfahrens authentifiziert.

30

4. Verfahren nach einem der Patentansprüche 1 bis 3,
dadurch gekennzeichnet,

daß die Kommunikation zwischen den Endgeräten und dem
Hintergrundsystem bzw. den Hintergrundsystemen der
jeweiligen Netzknoten erfolgt.

5. Verfahren nach einem der Patentansprüche 1 bis 4,
dadurch gekennzeichnet,

daß eine zusätzliche Führung der Geld- oder
Werteeinheiten, gegebenenfalls kryptographisch
gesichert, auf dem jeweiligen Datenträger zur
Durchführung einer Plausibilitätskontrolle erfolgt.

6. Verfahren nach einem der Patentansprüche 1 bis 5,
dadurch gekennzeichnet,

daß der in dem/den Hintergrundsystem(en) des Betreibers
hinterlegte geheime Schlüssel zu nur einem bestimmten
Datenträger vom Hintergrundsystem zur Entschlüsselung
der Antwort (Response) verwendet wird und

daß bei Übereinstimmung von Challenge und Response der
Datenträger als authentisch klassifiziert wird.

7. Verfahren nach einem der Patentansprüche 1 bis 6,
dadurch gekennzeichnet,

daß zum Erschweren des Scannens durch eine unbefugte
Person das Erkennungsmuster komplex ausgeführt wird.

1 / 1

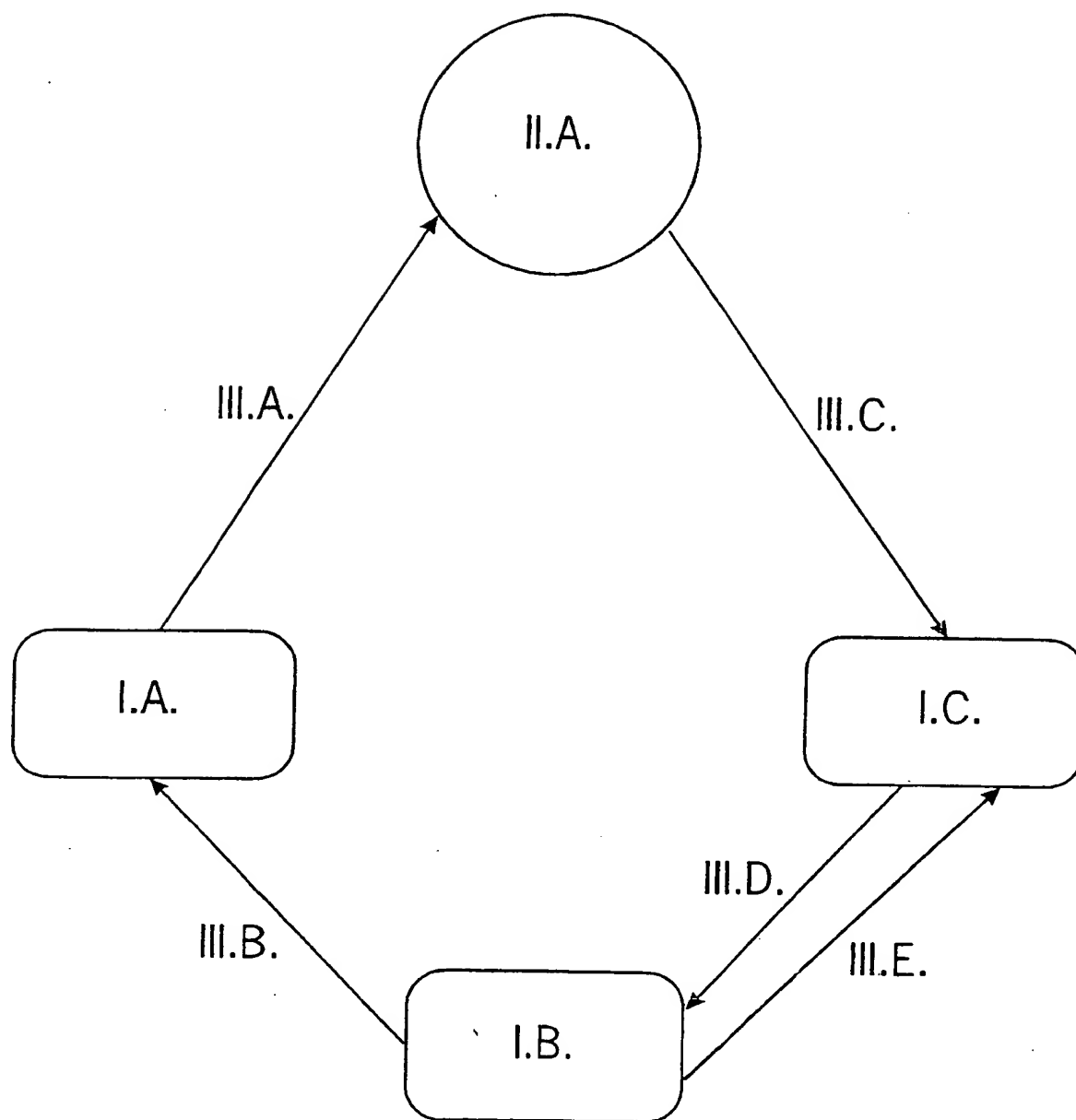


FIG. 1

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 99/09531

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G07F H04L H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 777 305 A (SMITH M BROOKS ET AL) 7 July 1998 (1998-07-07)	1
Y	abstract	5,7
Y	US 4 825 050 A (GRIFFITH JOHN B ET AL) 25 April 1989 (1989-04-25)	5
	abstract; claim 1; figure 1	
Y	EP 0 397 512 A (SHINSOZAI SOGO KENKYUSHO KK ;DAC INC (JP); NIHON CARD TRANSFER COR) 14 November 1990 (1990-11-14)	7
	abstract column 2, line 43 -column 3, line 16	
	-/-	

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"Z" document member of the same patent family

Date of the actual completion of the international search

28 February 2000

Date of mailing of the international search report

06/03/2000

Name and mailing address of the ISA

European Patent Office, P.B. 6818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3018

Authorized officer

Lindholm, A-M

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 99/09531

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 477 038 A (CLARK HELEN ET AL) 19 December 1995 (1995-12-19) abstract; figures 2,3 column 4, line 13 - line 66 column 6, line 45 -column 7, line 4	1,4
A	US 5 721 781 A (DEO VINAY ET AL) 24 February 1998 (1998-02-24) abstract	1,2
A	EP 0 654 919 A (SIEMENS AG) 24 May 1995 (1995-05-24) abstract; claim 1; figure 1	3,6
A	WO 98 52163 A (MONDEX INT LTD) 19 November 1998 (1998-11-19) abstract page 40, line 11 - line 18 page 42, line 19 -page 44, line 4	6

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 99/09531

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5777305	A	07-07-1998	NONE	
US 4825050	A	25-04-1989	NONE	
EP 0397512	A	14-11-1990	JP 2297297 A	07-12-1990
US 5477038	A	19-12-1995	AU 686276 B	05-02-1998
			AU 1039795 A	22-05-1995
			CA 2174951 A	04-05-1995
			CA 2258830 A	04-05-1995
			EP 0738404 A	23-10-1996
			JP 2897150 B	31-05-1999
			JP 9504396 T	28-04-1997
			WO 9512169 A	04-05-1995
			US RE36365 E	02-11-1999
US 5721781	A	24-02-1998	NONE	
EP 0654919	A	24-05-1995	DE 4339460 C	06-04-1995
WO 9852163	A	19-11-1998	AU 6299698 A	09-09-1998
			AU 7776798 A	08-12-1998
			AU 7776898 A	08-12-1998
			AU 7776998 A	08-12-1998
			AU 7777098 A	08-12-1998
			AU 7777198 A	08-12-1998
			AU 7777298 A	08-12-1998
			AU 7777398 A	08-12-1998
			AU 7777498 A	08-12-1998
			EP 0963580 A	15-12-1999
			EP 0976114 A	02-02-2000
			WO 9837526 A	27-08-1998
			WO 9852158 A	19-11-1998
			WO 9852159 A	19-11-1998
			WO 9852160 A	19-11-1998
			WO 9852161 A	19-11-1998
			WO 9852152 A	19-11-1998
			WO 9852162 A	19-11-1998
			WO 9852153 A	19-11-1998

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 99/09531

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 7 G07F7/10

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchiertes Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 G07F H04L H04M

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 777 305 A (SMITH M BROOKS ET AL) 7. Juli 1998 (1998-07-07)	1
Y	Zusammenfassung	5,7
Y	US 4 825 050 A (GRIFFITH JOHN B ET AL) 25. April 1989 (1989-04-25) Zusammenfassung; Anspruch 1; Abbildung 1	5
Y	EP 0 397 512 A (SHINSOZAI SOGO KENKYUSHO KK ;DAC INC (JP); NIHON CARD TRANSFER COR) 14. November 1990 (1990-11-14) Zusammenfassung Spalte 2, Zeile 43 -Spalte 3, Zeile 16	7
	-/-	

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"Z" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

28. Februar 2000

Abenddatum des internationalen Recherchenberichts

06/03/2000

Name und Postanschrift der internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3018

Bevollmächtigter Bediensteter

Lindholm, A-M

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 99/09531

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 477 038 A (CLARK HELEN ET AL) 19. Dezember 1995 (1995-12-19) Zusammenfassung; Abbildungen 2,3 Spalte 4, Zeile 13 - Zeile 66 Spalte 6, Zeile 45 - Spalte 7, Zeile 4	1,4
A	US 5 721 781 A (DEO VINAY ET AL) 24. Februar 1998 (1998-02-24) Zusammenfassung	1,2
A	EP 0 654 919 A (SIEMENS AG) 24. Mai 1995 (1995-05-24) Zusammenfassung; Anspruch 1; Abbildung 1	3,6
A	WO 98 52163 A (MONDEX INT LTD) 19. November 1998 (1998-11-19) Zusammenfassung Seite 40, Zeile 11 - Zeile 18 Seite 42, Zeile 19 - Seite 44, Zeile 4	6

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 99/09531

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
US 5777305	A	07-07-1998	KEINE		
US 4825050	A	25-04-1989	KEINE		
EP 0397512	A	14-11-1990	JP	2297297 A	07-12-1990
US 5477038	A	19-12-1995	AU	686276 B	05-02-1998
			AU	1039795 A	22-05-1995
			CA	2174951 A	04-05-1995
			CA	2258830 A	04-05-1995
			EP	0738404 A	23-10-1996
			JP	2897150 B	31-05-1999
			JP	9504396 T	28-04-1997
			WO	9512169 A	04-05-1995
			US	RE36365 E	02-11-1999
US 5721781	A	24-02-1998	KEINE		
EP 0654919	A	24-05-1995	DE	4339460 C	06-04-1995
WO 9852163	A	19-11-1998	AU	6299698 A	09-09-1998
			AU	7776798 A	08-12-1998
			AU	7776898 A	08-12-1998
			AU	7776998 A	08-12-1998
			AU	7777098 A	08-12-1998
			AU	7777198 A	08-12-1998
			AU	7777298 A	08-12-1998
			AU	7777398 A	08-12-1998
			AU	7777498 A	08-12-1998
			EP	0963580 A	15-12-1999
			EP	0976114 A	02-02-2000
			WO	9837526 A	27-08-1998
			WO	9852158 A	19-11-1998
			WO	9852159 A	19-11-1998
			WO	9852160 A	19-11-1998
			WO	9852161 A	19-11-1998
			WO	9852152 A	19-11-1998
			WO	9852162 A	19-11-1998
			WO	9852153 A	19-11-1998

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)